COUNTY COLLEGE OF MORRIS
MEASURES FOR IDENTITY THEFT PREVENTION

IDENTIFY, DETECT, RESPOND, REPORT, REVIEW

1. INDICATORS TO **IDENTIFY** RED FLAGS: Potential indicator of fraud:
   a. Notifications and warning from third-party agencies (i.e. credit agency).
   b. Suspicious documents including Identification (i.e. forgeries, altered documents, inconsistent statements).
   c. Unusual use of account (i.e. sudden change in password, mailing address, returned mail, breach in computer security).
   d. Student request made by a non-college issued email account.
   e. Request to mail something to an address not listed on the requestor's file.
   f. Notice from a student, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.

2. HOW TO **DETECT** THE RED FLAGS:
   a. Require identifying information (As established by your department) before providing access to records, whether online, over the phone, or in person.
   b. Verify identity of student/employee in person when possible.
   c. Verify significant changes in a student/employee account with the account holder.

3. HOW TO **RESPOND** TO THE RED FLAGS:
   a. Once detected, take one or more of the following steps in order to prevent and mitigate identity theft:

      i. Alert your supervisor and coordinate your response with the appropriate department as provided in part vii of this section.
      ii. Contact the student, applicant, or employee;
      iii. Change any passwords, security codes or other security devices that permit/prohibit access to the account;
      iv. Do not open a new account for the student/employee until the red flag has been cleared (Pertains to your duty to alert college offices to provide notice so that an alert can be placed in the student's/employee's account by the Information Systems Department, Bursar, Registrar, Human Resources, etc.);

v. Continue to monitor the account for evidence of identity theft for a reasonable period of time after detection (for example, an academic department would alert the Registrar and develop an internal process to "flag" the student's file as maintained by the department);
vi. Determine no response is warranted under the particular circumstance.
vii. IN ALL CASES, during the course of following CCM's Identity Theft Policy, notify one of the following officials in writing (and in all cases copy the Program Administrator – the Director of Budget & Compliance) to assess whether the attempted transaction was fraudulent; **Registrar** (for student account-related issues); **Bursar** (for student financial account-related issues); **Director of Financial Aid** (for student financial aid-related issues); **Director of Admissions** (for admission related issues); **Executive Director of Information Systems** (for data related issues); **Director of Human Resources and Labor Relations**(for employee account related issues); **Executive Director of College Advancement & Planning** (for donor and alumni related issues); **Vice President for Business & Finance** (for vendor and other customer related issues).

4. HOW TO **REPORT** INCIDENTS OF IDENTITY THEFT (INCLUDING ATTEMPTS OF IDENTITY THEFT)
   a. Upon the discovery of an incident and/or an attempt of identity theft, the manager/director of the office for which the discovery was made shall complete the Identity Theft Detection form which shall be submitted to the Program Administrator (Director of Budget and Compliance).
   b. The Identity Theft Detection form will be made available by contacting the Program Administrator.

5. **REVIEW** YOUR CURRENT PROCEDURES/PRACTICES
   a. Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with identifying or protected information (minimize hard copy storage whenever possible);
   b. Ensure that your departmental website, or related portal, is secure through consultation with the Information Systems Department;
   c. Follow college policies and procedures for data security when transmitting/storing protected information.
   d. Ensure complete and secure destruction of paper documents and computer files containing account information in accordance with the college's record retention policies and procedures;
   e. Ensure that all college computers, including servers, laptops, and desktops, are managed according to security best-practices. This includes restricting access through password protection, keeping the operating system updated with security patches and updates, running up-to-date virus detection software, and encrypting institutional data where required.

f. Sensitive institutional data should not be distributed via email or stored on external drives (USB, Thumb, Flash, etc.). Personally-owned drives and devices should never be used to store sensitive institutional data.
g. **Avoid the use of the social security number as an identifier and allow access to social security numbers to a very limited number of staff who have been approved by the Program Administrator.** As a best practice, it is also advisable to avoid using a combination of name, DOB, address for identification purposes.
h. Require and keep only information that is necessary for your business purpose.

The protection of student/employee information is the job of every employee at the college. These measures are meant to set the minimum requirements for an effective college response. Departments are encouraged to adopt more specific rules/procedures/protections to assist in the implementation of these measures. Please consult with the entire identity theft prevention policy, available from either the President's Office or Director of Budget and Compliance - Board Policy 2.2018.

If you have a question concerning these measures, reporting requirements or identify theft prevention in general, please contact the Director of Budget and Compliance (ext 5126).